UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

K.S., individually and on behalf of all others similarly situated, by his parent and guardian KWAJALYN SANDS. Plaintiff, v. MONTLICK & ASSOCIATES, P.C. Defendant.	**Case No.:** **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff K.S. ("Plaintiff"), by his parent and guardian Kwajalyn Sands, on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Montlick & Associates, P.C. ("Montlick" or "Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI") (collectively "Private Information") that was impacted in a data breach that

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

Defendant publicly disclosed on November 4, 2024 (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is a law firm based in Atlanta, Georgia.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. On September 2, 2024, Defendant became aware of a security incident impacting its IT Network.[3] Defendant took immediate steps and launched an investigation to determine the nature and scope of the Data Breach.[4]

6. Defendant's investigation confirmed that an unauthorized third-party gained access to its IT Network between August 15, 2024, and August 27, 2024, in which sensitive Private Information of clients and employees was compromised.[5]

7. Defendant then began a comprehensive review of the impacted data to determine what types of Private Information were compromised and how many individuals were impacted by the Data Breach. On October 7, 2024, Defendant completed its review.[6]

8. Upon information and belief, Defendant's investigation determined that the following types of Private Information was compromised in the Data

---

[2] *About,* Montlick & Associates, P.C. https://www.montlick.com/our-firm/ (last visited November 13, 2024).
[3] Exhibit 1
[4] *Id.*
[5] *Id.*
[6] *Id.*

Breach: full name, driver's license number, Social Security number, and medical information.[7]

9. On November 4, 2024, Defendant made a public disclosure of the Data Breach and started sending notice letters to impacted individuals.[8]

10. Defendant failed to take precautions designed to keep its clients' and employees' Private Information secure.

11. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

12. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

13. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

14. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

15. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer

---

[7] *Id.*
[8] *Id.*

injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

16. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

17. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence *per se*; unjust enrichment, breach of implied contract, and breach of confidence.

18. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

19. Plaintiff K.S., a minor, is a resident of Griffin, Georgia. Plaintiff K.S. received a notice letter from Defendant informing K.S. that their Private Information was compromised in the Data Breach.

Defendant

20. Defendant Montlick & Associates, P.C. is a law firm based in Atlanta, Georgia, having its principal place of business located at 17 Executive Park Dr NE, Atlanta, Georgia.

JURISDICTION AND VENUE

21. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class Members. Defendant has its principal place of business located in this District.

22. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in this District.

23. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

24. Montlick is a personal injury law firm based in Atlanta, Georgia.[9]

25. Upon information and belief, Defendant made promises and representations to its clients or employees,' including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[10]

---

[9] *About,* Montlick & Associates, P.C. https://www.montlick.com/our-firm/ (last visited November 13, 2024).

[10] *Privacy Policy*, Montlick & Associates, P.C. https://www.montlick.com/privacy-policy/ (last visited November 13, 2024). ("If you do provide Montlick &

26. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

28. On September 2, 2024, Defendant became aware of claims that information was taken from its IT Network.[11] Defendant took immediate steps and launched an investigation to determine the nature of the Data Breach.[12]

29. Defendant's investigation confirmed that an unauthorized third party gained access to its IT Network between August 15, 2024, and August 27, 2024, in which it obtained sensitive personal and protected health information of people in its computer network.[13]

30. Defendant then began a comprehensive review of the impacted data to determine what types of information were compromised and how many individuals were affected in the incident. On October 7, 2024, Defendant's review was completed.[14]

31. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised in the Data

---

Associates with Personal Information, Montlick & Associates will only use it for the purposes described where it is collected or to aggregate data in a manner that does not identify you, and Montlick & Associates will not sell, license, transmit or disclose this information outside of Montlick & Associates or its affiliates…").

[11] Exhibit 1

[12] *Id.*

[13] *Id.*

[14] *Id.*

Breach: full name, driver's license number, Social Security number, and medical information.[15]

32. On November 4, 2024, Montlick made a public disclosure of the Data Breach and started sending notice letters to impacted individuals.[16]

33. Plaintiff's claims arise from Defendant's failure to safeguard their Private Information and failure to provide timely notice of the Data Breach.

34. Defendant failed to take precautions designed to keep current and former clients' and employees' Private Information secure.

35. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

36. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

37. Defendant admits that unauthorized third persons accessed its network systems. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

38. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

---

[15] *Id.*
[16] *Id.*

39. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[17] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present clients' and employees' Private Information.

40. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[18] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

41. Here, Defendant waited nearly two months after being made aware of the Data Breach to notify impacted individuals.

D. The Harm Caused by the Data Breach Now and Going Forward

42. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[19]

43. The type of data that may have been accessed and compromised here – such as, names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

---

[17] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited November 13, 2024).

[18] *Id.*

[19] *Prevention and Preparedness*, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited November 13, 2024).

44. Plaintiff and Class Members face a substantial risk of identity theft given that their Social Security numbers and other important Private Information was compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

45. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

46. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[20]

47. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[21] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[22] As data breaches continue to reveal, "PII about employees, clients and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[23]

---

[20] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited November 13, 2024).

[21] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited November 13, 2024).

[22] *Id.*

[23] *Id.*

48. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[24] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[25]

49. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

50. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director of the cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[27]

---

[24] *Id.*

[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited November 13, 2024).

[26] *Id.*

[27] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited November 13, 2024).

51. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[28]

52. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[29] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant notified impacted people nearly two months after learning of the Data Breach.

53. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private

---

[28] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited November 13, 2024).

[29] *Id.*

Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

54. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

55. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

56. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

57. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States who were impacted by the Data Breach publicly announced by Defendant in November 2024 (the "Class").

58. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

59. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

60. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

61. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of hundreds of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

62. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had their Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and their claims are typical of the claims of the members of the Class.

The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

63. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

64. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

65. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure its past and present clients or employees' Private Information;

i. Whether Defendant was unjustly enriched; and

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

66. Information concerning Defendant's policies is available from Defendant's records.

67. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

68. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

69. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

70. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

71. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 70 as though fully set forth herein.

72. Plaintiff brings this claim individually and on behalf of the Class Members.

73. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

74. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

75. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

76. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its current and former clients or employees' Private Information.

77. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its clients and employees. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

78. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

79. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

80. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

81. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

82. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

83. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

84. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members'

Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

85. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

86. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

87. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

88. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

89. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

90. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal

information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 70 as though fully set forth herein.

92. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

93. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

94. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

95. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

96. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

97. As a result of Defendant's negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

98. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 70 as though fully set forth herein.

99. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their Private Information.

100. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information.

101. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

102. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

103. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 70 as though fully set forth herein.

104. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

105. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

106. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff sand Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

107. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

108. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

109. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

110. These exchanges constituted an agreement and meeting of the minds between the parties.

111. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

112. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

113. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

114. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

115. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

116. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 70 as though fully set forth herein.

118. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

119. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class

Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

120. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

121. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

122. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

123. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

124. As a direct and proximate cause of Defendant's actions and omissions, Plaintiff and the Class have suffered damages.

125. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

126. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known

its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

127. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former people; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

128. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 14, 2024

By: s/ *John C. Herman*_____

John C. Herman (Bar No. 347370)
Candace N. Smith (Bar No. 654910)
HERMAN JONES LLP
3424 Peachtree Road NE
Suite 1650
Atlanta, Georgia 30326
Telephone: 404-504-6555
Email: jherman@hermanjones.com
Email: csmith@hermanjones.com

Eduard Korsinsky*
Mark Svensson*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor

New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: ek@zlk.com
Email: msvensson@zlk.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice* forthcoming

EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Montlick & Associates, PC ("Montlick") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 2, 2024, Montlick identified malicious activity in its computer network. In response, Montlick promptly worked to isolate impacted systems, confirm the security of its network, and begin an investigation. The investigation determined that certain portions of Montlick's network were accessed between August 15, 2024 and August 27, 2024, and, during that timeframe, certain files were copied without authorization. As a result of that determination, Montlick initiated a comprehensive review of the files to determine what type of information was present and to whom it relates. This review was completed on October 7, 2024, and Montlick then worked to provide notice to potentially affected individuals as quickly as possible. The information identified in the reviewed files related to Maine residents varies by individual, and includes name, Social Security number, and driver's license number.

Notice to Maine Residents

On November 4, 2024, Montlick provided written notice of this incident to seventeen (17) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

In response to this event, Montlick moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals. Further, Montlick notified federal law enforcement regarding the event. Montlick is providing access to credit monitoring services for twelve (12) months, through Equifax, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

Additionally, Montlick is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Montlick is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

Montlick is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

MONTLICK
INJURY ATTORNEYS
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>:

Montlick & Associates, PC ("Montlick") is writing to notify you of an event that may affect some of your information. This notice provides you with information about this matter, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? On September 2, 2024, Montlick identified malicious activity in its computer network. In response, Montlick promptly worked to isolate impacted systems, confirm the security of its network, and begin an investigation. The investigation determined that certain portions of Montlick's network were accessed between August 15, 2024 and August 27, 2024, and, during that timeframe, certain files were copied without authorization. As a result of that determination, Montlick initiated a comprehensive review of the files to determine what type of information may have been present and to whom it relates. This review was completed on October 7, 2024, and we then worked to provide notice to potentially affected individuals as quickly as possible.

What Information Was Involved? While we have no evidence that any of your information has been used for identity theft or fraud, our investigation determined that the following information related to you may have been affected: name, Social Security number, and driver's license number. For a small number of individuals, medical treatment and/or diagnosis information may be included.

What We Are Doing. In response to this matter, we dedicated significant resources to confirming the security of our network, conducting a comprehensive investigation, and completing a detailed review of the relevant files. We then worked to provide notice to potentially affected individuals as quickly as possible. As part of our ongoing commitment to the security of information in our care, we are also reviewing our existing policies and procedures and enhancing our existing security tools.

As an added precaution, we are offering you <<CM Duration>> months of credit monitoring and identity protection services, through Equifax, at no cost to you. If you wish to activate these services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information* section on the next page of this letter. Please note you must enroll in these services directly, as we are unable to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Again, additional information and resources may be found in the *Steps You Can Take to Help Protect Personal Information* section on the next page of this letter.

For More Information. If you have additional questions regarding this incident, please call our dedicated call center at 855-278-0571, which is available 9 am to 9 pm Eastern, Monday through Friday (excluding holidays).

Sincerely,

Montlick & Associates

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

EQUIFAX®

<<Full Name>>
Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. *[2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com* *[4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. You may write to Montlick at 17 Executive Park Drive, Suite 300, Atlanta, GA 30029.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.